



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,814	03/14/2005	Jarmo Talvitie	3502-1075	4622
466	7590	08/23/2007		
YOUNG & THOMPSON 745 SOUTH 23RD STREET 2ND FLOOR ARLINGTON, VA 22202			EXAMINER AVERY, JEREMIAH L	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 08/23/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

mn

<b>Office Action Summary</b>	<b>Application No.</b> 10/527,814	<b>Applicant(s)</b> TALVITIE, JARMO	
	<b>Examiner</b> Jeremiah Avery	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 01 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-6, 8-23 and 25-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-23 and 25-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 March 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 7, 24 and 38 have been cancelled.
2. Claims 1-6, 8-23 and 25-37 have been examined.
3. Responses to Applicant's remarks have been given.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "quicker" in claim 8 is a relative term which renders the claim indefinite. The term "quicker" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6, 8-23 and 25-37 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication No. US 2002/0116639 to Chefalas et al., hereinafter Chefalas.

Art Unit: 2131

2. Regarding claim 1, Chefalas discloses a security system for repelling viruses in computers and computer networks and that is adapted to forward messages, the security system comprising a first sub-system (1) to detect unknown viruses, said first sub-system being adapted in connection with the forwarding of messages or with other action or, in a timed manner, to perform one or more predetermined actions to activate unknown viruses and to detect the activated unknown viruses by detecting consequences of virus activation (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 30 and 32, page 4, paragraph 46 and page 5, paragraph 54).
3. Regarding claim 2, Chefalas discloses the security system in accordance with claim 1, that is adapted to forward an alarm caused by the detection of a virus to at least one system connected to the security system page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 30 and 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108" and page 4, paragraph 46).
4. Regarding claim 3, Chefalas discloses the security system in accordance with claim 1, that is further adapted to break a connection to at least one other system on the basis of an alarm caused by the detection of a virus (page 1, paragraph 12, page 2,

remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraph 30 and page 4, paragraph 46).

5. Regarding claim 4, Chefalas discloses a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

6. Regarding claim 5, Chefalas discloses a third sub-system that is adapted to break a connection to at least one other sub-system upon receiving an alarm (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraph 30, page 4, paragraph 46 and page 5, paragraph 54).

7. Regarding claim 6, Chefalas discloses wherein the at least one other sub-system includes an identifier which corresponds to an identifier of the third sub-system (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

8. Regarding claim 8, Chefalas discloses wherein the alarm is a message or at least a part of a message that is forwarded to the recipient quicker than other communications (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client

Art Unit: 2131

112 and all other clients connected to the server” and page 3, remainder of paragraph 28).

9. Regarding claim 9, Chefalas discloses wherein the third sub-system includes at least one computer or one network element including a computer (page 3, paragraph 32, “If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108”).

10. Regarding claim 10, Chefalas discloses wherein the alarm is forwarded via a separate connection (page 1, paragraph 12 and page 3, paragraph 32, “If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108”).

11. Regarding claim 11, Chefalas discloses wherein the one or more predetermined actions include at least one of altering the time data, altering the contents of the memory, handling of files or at least its partial simulation (page 4, paragraph 44).

12. Regarding claim 12, Chefalas discloses wherein the consequences of virus activation detected by the first sub-system include at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a virus, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

Art Unit: 2131

13. Regarding claim 13, 27 and 35, Chefalas discloses wherein the one or more predetermined actions include plural actions that take place either simultaneously or consecutively in time (page 4, paragraph 46).

14. Regarding claim 14, 28 and 36, Chefalas discloses wherein the first sub-system is adapted to choose one or more of the following logics when trying to activate viruses: one defined by the user, pre-programmed or at least partially random logic (page 5, paragraph 60).

15. Regarding claim 15, Chefalas discloses further comprising a parallel system that is adapted to save a message sent from the third sub-system, the parallel system being connected in parallel with the third sub-system (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

16. Regarding claim 16, Chefalas discloses wherein the first sub-system is adapted to compare in the parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a virus (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

17. Regarding claim 17, Chefalas discloses wherein the parallel system is adapted to forward a message saved by it (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

18. Regarding claim 18, Chefalas discloses the security system in accordance with claim 1, that is adapted to examine messages forwarded through the security system in

order to detect known viruses (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

19. Regarding claim 19, Chefalas discloses the security system in accordance with claim 4, comprising first and second ones of the at least one system, wherein the security system is adapted to transfer data between the first and the second ones of the at least one system through the first and the second sub-systems, and wherein the security system is adapted to disrupt the connection between the first one of the at least one system and the first sub-system before a connection is established between the first and the second sub-systems and to disrupt the connection between the first and the second sub-systems before a connection is established between the second sub-system and the second one of the at least one system (page 1, paragraph 12, page 3, paragraph 30, "shut down the local server and/or the LAN" and page 5, paragraph 54).

20. Regarding claim 20, Chefalas discloses wherein said first sub-system is adapted to compare messages with at least partially identical identifiers with each other in order to detect unknown viruses (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

21. Regarding claim 21, Chefalas discloses wherein the first sub-system is adapted to request the sender of the messages with at least partially identical identifiers to re-send at least one of the messages and is further adapted to compare at least one re-sent message received with the original messages in order to detect messages containing viruses (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).



22. Regarding claim 22, Chefalas teaches a method for repelling viruses in computers and data networks, the method being carried out in a security system including a first sub-system for forwarding messages and for detecting viruses and that is isolatable from the remainder of the security system (page 1, paragraph 12, page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30, "shut down the local server and/or the LAN"), the method includes the steps where: functions of the security system are monitored by the first sub-system in order to detect consequences of activation of an unknown virus (page 1, paragraph 12, page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30), the consequences of activation including at least one of the following: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a virus, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there, a virus is detected when one of the consequences is detected, and an alarm is given (page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30).

23. Regarding claim 23, Chefalas teaches a method for repelling viruses in computers and computer networks, the method comprising the steps of: taking one of more predetermined actions to activate unknown viruses in connection with the forwarding of messages or other action, or in a timed manner, detecting the

activated unknown viruses by detecting consequences of virus activation caused by the one or more predetermined actions, and giving an alarm when a virus is detected (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28 and page 3, remainder of paragraph 28 and paragraphs 29 and 30).

24. Regarding claims 25 and 32, Chefalas teaches A method in accordance with claim 23, wherein the one or more predetermined actions include at least one of the following: altering the time data, altering the contents of the memory, handling of files or at least its partial simulation (page 5, paragraphs 50 and 60).

25. Regarding 26, Chefalas teaches wherein the method is run in a security system including a first sub-system and a second sub-system and wherein the consequences of virus activation include at least one of:

a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a virus, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraphs 25 and 28, page 3, remainder of paragraph 28 and paragraphs 30-32, page 4, paragraphs 44, 46 and 47 and page 5, paragraph 54).

26. Regarding claim 29, Chefalas teaches further comprising the step where known viruses are searched for on the basis of their characteristics (page 3, paragraph 32, "If

the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

27. Regarding claim 30, Chefalas teaches wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system and the second system through the first sub-system and the second sub-system phase by phase in order (page 1, paragraph 12 and page 5, paragraph 54), in which phases:

the connection for data transfer is disrupted between the first system and the first sub-system, a connection for data transfer is established between the first sub-system and the second sub-system, the connection for data transfer is disrupted between the first sub-system and the second sub-system, a connection for data transfer is established between the second sub-system and the second system (page 5, paragraph 54).

28. Regarding claim 31, Chefalas discloses an apparatus for repelling viruses in computers and computer networks, comprising equipment for saving data and for handling data and equipment for transferring data with another apparatus, wherein the apparatus is adapted to receive a message and to perform one or more predetermined actions to activate unknown viruses contained in the message and to detect the activated unknown viruses by detecting consequences of virus activation (page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30).

29. Regarding claim 33, Chefalas discloses wherein the consequences of virus activation include at least one of: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the

Art Unit: 2131

apparatus to detect a virus (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraphs 23 and 27).

30. Regarding claim 34, Chefalas discloses wherein the apparatus is adapted to send a message to either a sub-assembly of the apparatus or to said another apparatus (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108"), and wherein the consequences of virus activation include at least one of:

a message leaves without authorization from the anti-virus software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent (page 2, paragraphs 25 and 28, page 3, remainder of paragraph 28 and paragraphs 30-32 and page 4, paragraphs 44, 46 and 47).

31. Regarding claim 37, Chefalas discloses wherein the apparatus examines the message in order to detect known viruses (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

***Response to Arguments***

32. The cancellation of claim 38 renders the 35 U.S.C. 112, 2<sup>nd</sup> paragraph of said claim to be moot and is thus withdrawn.

33. Applicant's arguments filed 06/01/07 have been fully considered but they are not persuasive. The Examiner maintains the above-cited grounds of rejection. Further, with regards to the claim of "unknown viruses", the Examiner maintains that Chefalas discloses this, in particular but not limited to, on page 5, paragraphs 50 and 54. A virus is detected, but is not clarified if it is a previously-known virus, thus it is broadly interpreted by the Examiner that a detection of a virus, but not as to whether it has been detected previously renders the detected virus as a new or "unknown" virus.

***Conclusion***

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

35. The following United States Patents are cited to further show the state of the art with respect to virus detection and removal, such as:

United States Patent No. 7,137,034 to Largman et al., which is cited to show a self repairing computer having user accessible switch for modifying bootable storage device configuration to initiate repair.

United States Patent No. 6,873,988 to Hermann et al., which is cited to show system and methods providing anti-virus cooperative enforcement.

36. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2131

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

37. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

40. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA

CHRISTOPHER REVAK  
PRIMARY EXAMINER

